

EXHIBIT 9

RS Switch Router User Guide

Release 7.0

36-007-03 Rev. 0A



COPYRIGHT NOTICES

© 2001 by Riverstone Networks, Inc. All rights reserved.

Riverstone Networks, Inc.
5200 Great America Parkway
Santa Clara, CA 95054

Printed in the United States of America

This product includes software developed by the University of California, Berkeley, and its contributors.

© 1979 – 1994 by The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley, and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Changes

Riverstone Networks, Inc., and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Riverstone Networks, Inc., to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

Disclaimer

IN NO EVENT SHALL RIVERSTONE NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF RIVERSTONE NETWORKS HAS BEEN ADVISED, KNOWN, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks

Riverstone Networks, Riverstone, RS, and IA are trademarks of Riverstone Networks, Inc.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

TABLE OF CONTENTS

1	Introduction	1-1
1.1	Related Documentation	1-1
1.2	Document Conventions	1-2
2	Maintaining Configuration Files	2-1
2.1	Configuration Files	2-1
2.1.1	Changing Configuration Information	2-2
2.1.2	Displaying Configuration Information	2-2
2.1.3	Activating the Configuration Commands in the Scratchpad	2-3
2.1.4	Saving the Active Configuration to the Startup Configuration File	2-4
2.1.5	Viewing the Current Configuration	2-4
2.1.6	Backing Up and Restoring Configuration Files	2-5
2.2	Backing Up and Restoring System Image Files	2-6
2.3	Configuring System Settings	2-7
2.3.1	Setting Daylight Saving Time	2-8
2.3.2	Configuring a Log-in Banner	2-8
3	Using the CLI	3-1
3.1	Command Modes	3-1
3.1.1	User Mode	3-1
3.1.2	Enable Mode	3-1
3.1.3	Configure Mode	3-2
3.1.4	Boot PROM Mode	3-2
3.2	Establishing Telnet Sessions	3-2
3.3	Setting CLI Parameters	3-3
3.4	Getting Help with CLI Commands	3-4
3.5	Line Editing Commands	3-6
3.6	Port Names	3-8
4	Hot Swapping Line Cards and Control Modules	4-1
4.1	Hot Swapping Overview	4-1
4.2	Hot Swapping Line Cards	4-1
4.2.1	Deactivating the Line Card	4-2
4.2.2	Removing the Line Card	4-2
4.2.3	Installing a New Line Card	4-3
4.3	Hot Swapping One Type of Line Card With Another	4-3
4.4	Hot Swapping a Secondary Control Module	4-3
4.4.1	Deactivating the Control Module	4-4

4.4.2	Removing the Control Module	4-5
4.4.3	Installing a Control Module	4-5
4.5	Hot Swapping a Switching Fabric Module (RS 8600 only)	4-5
4.5.1	Removing the Switching Fabric Module	4-6
4.5.2	Installing a Switching Fabric Module	4-6
4.6	Hot Swapping A GBIC (RS 32000 and RS 38000 only)	4-7
4.6.1	Removing a GBIC from the Line Card	4-7
4.6.2	Installing a GBIC into the Line Card	4-8
4.7	Hot Swapping a WIC	4-8
5	Bridging Configuration Guide	5-1
5.1	Spanning Tree (IEEE 802.1d)	5-1
5.2	Bridging Modes (Flow-Based and Address-Based)	5-1
5.3	VLAN Overview	5-2
5.3.1	RS VLAN Support	5-3
5.3.2	Configuration Examples	5-4
5.4	Access Ports and Trunk Ports (802.1P and 802.1Q support)	5-5
5.5	Configuring RS Bridging Functions	5-6
5.5.1	Configuring Address-based or Flow-based Bridging	5-6
5.6	Configuring Spanning Tree	5-7
5.6.1	Using Rapid STP	5-7
5.6.2	Adjusting Spanning-Tree Parameters	5-8
5.6.3	STP Dampening	5-11
5.7	Configuring a Port- or Protocol-Based VLAN	5-11
5.7.1	Creating a Port or Protocol Based VLAN	5-12
5.7.2	Adding Ports to a VLAN	5-12
5.7.3	Configuring VLAN Trunk Ports	5-12
5.8	Configuring VLANs for Bridging	5-12
5.9	Configuring Layer-2 Filters	5-13
5.10	Monitoring Bridging	5-13
5.11	GARP/GVRP	5-14
5.11.1	Running GARP/GVRP with STP	5-14
5.11.2	Configuring GARP/GVRP	5-15
5.11.3	Configuration Example	5-16
5.12	Tunneling VLAN packets across MANs	5-18
5.12.1	Stackable VLAN Components	5-18
5.12.2	Configuration Examples	5-19
5.12.3	Displaying Stackable VLAN Information	5-34
6	SmartTRUNK Configuration Guide	6-1
6.1	Overview	6-1
6.2	Configuring SmartTRUNKS	6-1
6.2.1	Creating a SmartTRUNK	6-2
6.2.2	Add Physical Ports to the SmartTRUNK	6-2
6.3	Monitoring SmartTRUNKS	6-3

6.4	SmartTRUNK Example Configuration.	6-4
6.5	Configuring the Link Aggregation Control Protocol (LACP)	6-5
6.5.1	Configuring SmartTRUNKs for LACP	6-5
6.5.2	LACP Configuration Example.	6-6
7	CMTS Configuration.	7-1
7.1	HFC Cable Network Architecture.	7-1
7.2	CMTS line card Description	7-2
7.3	Provisioning the Headend	7-3
7.4	Headend Certification	7-3
7.5	IF-RF-Upconverter	7-3
7.6	Diplex Filters.	7-4
7.7	DHCP, DNS, and TFTP Servers.	7-5
7.8	Connecting and Configuring the Downstream	7-6
7.8.1	Installing and Configuring the Upconverter	7-6
7.8.2	Setting the Upconverter Input Level	7-6
7.8.3	Setting the Upconverter Output Level	7-6
7.8.4	Setting the Upconverter Output Frequency	7-7
7.8.5	Completing the Downstream Configuration	7-7
7.8.6	Testing the Downstream Configuration.	7-7
7.9	Connecting the Upstream to the Laser Receiver.	7-8
7.10	Configuring the RS 8000/8600 CMTS line card.	7-8
7.10.1	Configuring the CMTS line card in a Bridged Network	7-8
7.10.2	Configuring the CMTS line card in a Routed Network.	7-9
7.11	Configuration Examples	7-10
7.11.1	Example 1: Multiple ISPs share a single DHCP server.	7-11
7.11.2	Example 2: Multiple ISPs with multiple DHCP servers	7-14
7.11.3	Example 3: Overlapping VLANs with multiple DHCP servers	7-18
8	ATM Configuration Guide.	8-1
8.1	Virtual Channels	8-2
8.1.1	Creating a Virtual Channel	8-2
8.1.2	Setting the Operation Mode for a Virtual Channel	8-2
8.1.3	Clearing Statistics on a Virtual Channel	8-3
8.2	Virtual Channel Groups	8-4
8.2.1	Creating a Virtual Channel Group	8-4
8.2.2	Adding a VC to a Virtual Channel Group	8-4
8.2.3	Setting the Operation Mode for a Virtual Channel Group.	8-5
8.3	Service Profile.	8-6
8.3.1	Creating a Service Profile	8-6
8.3.2	Applying a Service Profile to a Virtual Channel	8-8
8.3.3	Applying a Service Profile to a Virtual Channel Group	8-9
8.4	Cell Scrambling.	8-10
8.4.1	Enabling Cell Scrambling	8-10
8.5	Cell Mapping.	8-10
8.5.1	Selecting the Cell Mapping Format	8-11

8.6	VPI Bit Allocation	8-11
8.6.1	Setting the Bit Allocation for VPI	8-12
8.7	Peer Address Mapping	8-12
8.7.1	Mapping a Peer Address to a Virtual Channel	8-13
8.8	Configuring SONET Parameters	8-13
8.9	Automatic Protection Switching (APS)	8-14
8.9.1	Configuring APS	8-14
8.10	Displaying ATM Port Information	8-15
8.11	ATM sample configurations	8-20
8.11.1	ATM Sample Configuration 1	8-21
8.11.2	ATM Sample Configuration 2	8-24
8.11.3	ATM Sample Configuration 3	8-30
8.11.4	ATM Sample Configuration 4	8-33
8.11.5	ATM Sample Configuration 5	8-38
8.11.6	ATM Sample Configuration 6	8-41
8.11.7	Apply the Service Profile	8-41
8.11.8	Configure the AAA Server	8-42
9	Packet-over-SONET Configuration Guide	9-1
9.1	Configuring IP Interfaces for PoS Links	9-1
9.2	Configuring Packet-over-SONET Links	9-2
9.3	Configuring Automatic Protection Switching	9-3
9.3.1	Configuring Working and Protecting Ports	9-3
9.4	Specifying Bit Error Rate Thresholds	9-5
9.5	Monitoring PoS Ports	9-6
9.6	Example Configurations	9-6
9.6.1	APS PoS Links Between RS's	9-7
9.6.2	PoS Link Between the RS and a Cisco Router	9-7
9.6.3	PoS Link Between the RS and a Juniper Router	9-8
9.6.4	Bridging and Routing Traffic Over a PoS Link	9-9
9.6.5	PoS Link Through a Layer 2 Cloud	9-9
10	DHCP Configuration Guide	10-1
10.1	Configuring DHCP	10-1
10.1.1	Configuring an IP Address Pool	10-2
10.1.2	Configuring Client Parameters	10-2
10.1.3	Configuring a Static IP Address	10-3
10.1.4	Grouping Scopes with a Common Interface	10-3
10.1.5	Configuring DHCP Server Parameters	10-3
10.2	Updating the Lease Database	10-3
10.3	Monitoring the DHCP Server	10-4
10.4	DHCP Configuration Examples	10-4
10.5	Configuring Secondary Subnets	10-5
10.6	Secondary Subnets and Directly-Connected Clients	10-6
10.7	Interacting with Relay Agents	10-7

11	IP Routing Configuration Guide	11-1
11.1	IP Routing Protocols	11-1
11.1.1	Unicast Routing Protocols	11-1
11.1.2	Multicast Routing Protocols	11-1
11.2	Configuring IP Interfaces and Parameters	11-2
11.2.1	Configuring IP Interfaces to Ports	11-2
11.2.2	Configuring IP Interfaces for a VLAN	11-3
11.2.3	Specifying Ethernet Encapsulation Method	11-3
11.2.4	Unnumbered Interfaces	11-3
11.3	Configuring Jumbo Frames	11-3
11.4	Configuring Address Resolution Protocol (ARP)	11-4
11.4.1	Configuring ARP Cache Entries	11-4
11.4.2	Unresolved MAC Addresses for ARP Entries	11-5
11.4.3	Configuring Proxy ARP	11-5
11.5	Configuring Reverse Address Resolution Protocol (RARP)	11-6
11.5.1	Specifying IP Interfaces for RARP	11-6
11.5.2	Defining MAC-to-IP Address Mappings	11-6
11.5.3	Monitoring RARP	11-7
11.6	Configuring DNS Parameters	11-7
11.7	Configuring IP Services (ICMP)	11-7
11.8	Configuring IP Helper	11-7
11.9	Configuring Direct Broadcast	11-8
11.10	Configuring Denial of Service (DOS)	11-8
11.11	Monitoring IP Parameters	11-9
11.12	Configuring IP Forwarding	11-10
11.13	Hardware Routing Table	11-11
11.14	Configuring ICMP Redirect	11-11
11.15	Forwarding Mode	11-11
11.15.1	Configuring Destination-Based and Host-Flow-Based Forwarding	11-12
11.15.2	Configuring a Custom Forwarding Profile	11-12
11.15.3	Monitoring Custom Forwarding Profiles	11-13
11.15.4	Using Custom Forwarding with Other RS Features	11-13
11.16	Configuring Router Discovery	11-14
11.17	Setting Memory Thresholds	11-16
11.18	Configuration Examples	11-18
11.18.1	Assigning IP/IPX Interfaces	11-18
12	VRRP Configuration Guide	12-1
12.1	Configuring VRRP	12-1
12.1.1	Basic VRRP Configuration	12-2
12.1.2	Symmetrical Configuration	12-3
12.1.3	Multi-Backup Configuration	12-5
12.2	Additional Configuration	12-9
12.2.1	Setting the Backup Priority	12-9
12.2.2	Setting the Warmup Period	12-9

12.2.3	Setting the Advertisement Interval	12-9
12.2.4	Setting Pre-empt Mode	12-10
12.2.5	Setting an Authentication Key	12-10
12.3	Monitoring VRRP	12-10
12.3.1	ip-redundancy trace	12-11
12.3.2	ip-redundancy show	12-11
12.4	VRRP Configuration Notes	12-13
13	RIP Configuration Guide	13-1
13.1	Configuring RIP	13-1
13.1.1	Enabling and Disabling RIP	13-1
13.1.2	Configuring RIP Interfaces	13-1
13.2	Configuring RIP Parameters	13-2
13.2.1	Configuring RIP Route Default-Metric	13-4
13.3	Monitoring RIP	13-4
13.4	Configuration Example	13-5
14	OSPF Configuration Guide	14-1
14.1	OSPF Multipath	14-2
14.2	Configuring OSPF	14-2
14.3	Setting the Router ID	14-2
14.4	Enabling OSPF	14-3
14.5	Configuring OSPF Areas	14-3
14.5.1	Configuring Summary Ranges	14-4
14.5.2	Configuring Stub Areas	14-4
14.5.3	Configuring Not-So-Stubby Areas (NSSA)	14-5
14.6	Configuring OSPF Interfaces	14-6
14.6.1	Configuring Interfaces for NBMA Networks	14-6
14.6.2	Configuring Interfaces for Point-to-Multipoint Networks	14-7
14.6.3	Configuring Interfaces for Point-to-Point Networks	14-7
14.7	Configuring OSPF Interface Parameters	14-7
14.7.1	Setting the Interface State	14-8
14.7.2	Setting the Default Cost of an OSPF Interface	14-8
14.8	Creating Virtual Links	14-8
14.9	Configuring OSPF Parameters	14-9
14.9.1	Configuring OSPF Global Parameters	14-10
14.10	Monitoring OSPF	14-12
14.11	OSPF Configuration Examples	14-14
14.11.1	Exporting All Interface & Static Routes to OSPF	14-15
14.11.2	Exporting All RIP, Interface & Static Routes to OSPF	14-15
15	IS-IS Configuration Guide	15-1
15.1	Defining an IS-IS Area	15-1
15.2	Configuring IS-IS Interfaces	15-1

15.3	Enabling IS-IS on the RS	15-2
15.4	Setting IS-IS Global Parameters	15-2
15.4.1	Setting the IS Operating Level	15-2
15.4.2	Setting the PSN Interval	15-2
15.4.3	Setting the System ID	15-3
15.4.4	Setting the SPF Interval	15-3
15.4.5	Setting the Overload Bit	15-3
15.4.6	Setting IS-IS Authentication	15-4
15.5	Setting IS-IS Interface Parameters	15-5
15.5.1	Setting the Interface Operating Level	15-5
15.5.2	Setting Interface Parameters for a Designated Intermediate System (DIS)	15-6
15.5.3	Setting IS-IS Interface Timers	15-6
15.6	Displaying IS-IS Information	15-6
15.6.1	IS-IS Sample Configuration	15-7
16	BGP Configuration Guide	16-1
16.1	The RS BGP Implementation	16-1
16.2	Basic BGP Tasks	16-2
16.2.1	Setting the Autonomous System Number	16-2
16.2.2	Setting the Router ID	16-2
16.2.3	Configuring a BGP Peer Group	16-3
16.2.4	Adding and Removing a BGP Peer	16-4
16.2.5	Starting BGP	16-4
16.2.6	Using AS-Path Regular Expressions	16-4
16.2.7	Using the AS Path Prepend Feature	16-6
16.2.8	Creating BGP Confederations	16-7
16.2.9	Creating Community Lists	16-8
16.2.10	Using Route Maps	16-8
16.2.11	Using BGP Accounting	16-11
16.3	BGP Configuration Examples	16-13
16.3.1	BGP Peering Session Example	16-14
16.3.2	IBGP Configuration Example	16-16
16.3.3	EBGP Multihop Configuration Example	16-18
16.3.4	Community Attribute Example	16-22
16.3.5	Local Preference Examples	16-28
16.3.6	Multi-Exit Discriminator Attribute Example	16-31
16.3.7	EBGP Aggregation Example	16-32
16.3.8	Route Reflection Example	16-33
16.3.9	BGP Confederation Example	16-36
16.3.10	Route Map Example	16-41
16.3.11	BGP Accounting Examples	16-42
17	MPLS Configuration	17-1
17.1	Configuring a Static Label Switched Path	17-1
17.2	Static LSP Example	17-2
18	Routing Policy Configuration	18-1
18.1	Preference	18-1

18.1.1	Import Policies	18-2
18.1.2	Export Policies	18-3
18.1.3	Specifying a Route Filter	18-4
18.1.4	Aggregates and Generates	18-5
18.1.5	Authentication	18-6
18.2	Configuring Simple Routing Policies	18-7
18.2.1	Redistributing Static Routes	18-8
18.2.2	Redistributing Directly Attached Networks	18-8
18.2.3	Redistributing RIP into RIP	18-8
18.2.4	Redistributing RIP into OSPF	18-9
18.2.5	Redistributing OSPF to RIP	18-9
18.2.6	Redistributing Aggregate Routes	18-9
18.2.7	Simple Route Redistribution Example: Redistribution into RIP	18-10
18.2.8	Simple Route Redistribution Example: Redistribution into OSPF	18-11
18.3	Configuring Advanced Routing Policies	18-13
18.3.1	Export Policies	18-13
18.3.2	Creating an Export Destination	18-15
18.3.3	Creating an Export Source	18-15
18.3.4	Import Policies	18-15
18.3.5	Creating an Import Source	18-16
18.3.6	Creating a Route Filter	18-16
18.3.7	Creating an Aggregate Route	18-16
18.3.8	Creating an Aggregate Destination	18-17
18.3.9	Creating an Aggregate Source	18-17
18.3.10	Import Policies Example: Importing from RIP	18-18
18.3.11	Import Policies Example: Importing from OSPF	18-21
18.3.12	Export Policies Example: Exporting to RIP	18-24
18.3.13	Export Policies Example: Exporting to OSPF	18-29
19	Multicast Routing Configuration	19-1
19.1	IGMP Overview	19-1
19.2	DVMRP Overview	19-1
19.3	Configuring IGMP	19-2
19.3.1	Configuring IGMP on an IP Interface	19-2
19.3.2	Configuring IGMP Query Interval	19-3
19.3.3	Configuring IGMP Response Wait Time	19-3
19.3.4	Configuring Per-Interface Control of IGMP Membership	19-3
19.3.5	Configuring Static IGMP Groups	19-3
19.4	Configuring DVMRP	19-4
19.4.1	Starting and Stopping DVMRP	19-4
19.4.2	Configuring DVMRP on an Interface	19-4
19.4.3	Configuring DVMRP Parameters	19-4
19.4.4	Configuring the DVMRP Routing Metric	19-5
19.4.5	Configuring DVMRP TTL & Scope	19-5
19.4.6	Configuring a DVMRP Tunnel	19-6
19.5	Monitoring IGMP & DVMRP	19-6
19.6	Configuration Example	19-7
20	IP Policy-Based Forwarding Configuration	20-1

20.1	Configuring IP Policies	20-1
20.1.1	Defining an ACL Profile	20-2
20.1.2	Associating the Profile with an IP Policy	20-2
20.1.3	Applying an IP Policy to an Interface	20-5
20.2	IP Policy Configuration Examples	20-5
20.2.1	Routing Traffic to Different ISPs.	20-6
20.2.2	Prioritizing Service to Customers	20-7
20.2.3	Authenticating Users through a Firewall	20-8
20.2.4	Firewall Load Balancing	20-9
20.3	Monitoring IP Policies	20-11
21	Network Address Translation Configuration.	21-1
21.1	Configuring NAT	21-1
21.1.1	Setting Inside and Outside Interfaces.	21-2
21.1.2	Setting NAT Rules.	21-2
21.2	Forcing Flows through NAT	21-2
21.3	Managing Dynamic Bindings	21-3
21.4	NAT and DNS.	21-3
21.5	NAT and ICMP Packets	21-4
21.6	NAT and FTP	21-4
21.7	Monitoring NAT	21-5
21.8	Configuration Examples	21-5
21.8.1	Static Configuration	21-5
21.8.2	Dynamic Configuration	21-7
21.8.3	Dynamic NAT with IP Overload (PAT) Configuration.	21-8
21.8.4	Dynamic NAT with DNS.	21-9
21.8.5	Dynamic NAT with Outside Interface Redundancy	21-11
22	Web Hosting Configuration	22-1
22.1	Overview	22-1
22.2	Load Balancing	22-2
22.2.1	Creating the Server Group	22-2
22.2.2	Adding Servers to a Load Balanced Group	22-5
22.2.3	Optional Group or Server Operating Parameters.	22-6
22.2.4	Displaying Load Balancing Information	22-12
22.2.5	Load Balancing Configuration Examples	22-19
22.3	Web Caching.	22-25
22.3.1	Configuring Web Caching.	22-25
22.3.2	Additional Web Caching Options	22-28
22.3.3	Displaying Web-Caching Information.	22-31
22.3.4	Web Caching Configuration Examples	22-34
23	IPX Routing Configuration	23-1
23.1	RIP (Routing Information Protocol)	23-1
23.2	SAP (Service Advertising Protocol)	23-2

23.3	Configuring IPX RIP & SAP	23-2
23.3.1	IPX RIP	23-2
23.3.2	IPX SAP	23-2
23.3.3	Creating IPX Interfaces	23-2
23.3.4	IPX Addresses	23-3
23.4	Configuring IPX Interfaces and Parameters	23-3
23.4.1	Configuring IPX Addresses to Ports	23-3
23.4.2	Configuring Secondary Addresses on an IPX Interface	23-3
23.4.3	Configuring IPX Interfaces for a VLAN	23-4
23.4.4	Specifying IPX Encapsulation Method	23-4
23.5	Configuring IPX Routing	23-5
23.5.1	Enabling IPX RIP	23-5
23.5.2	Enabling SAP	23-5
23.5.3	Configuring Static Routes	23-5
23.5.4	Configuring Static SAP Table Entries	23-5
23.5.5	Controlling Access to IPX Networks	23-6
23.6	Monitoring an IPX Network	23-8
23.7	Configuration Examples	23-8
24	Access Control List Configuration	24-1
24.1	ACL Basics	24-1
24.1.1	Defining Selection Criteria in ACL Rules	24-1
24.1.2	How ACL Rules are Evaluated	24-3
24.1.3	Implicit Deny Rule	24-4
24.1.4	Allowing External Responses to Established TCP Connections	24-5
24.2	Creating and Modifying ACLs	24-6
24.2.1	Editing ACLs Offline	24-6
24.2.2	Maintaining ACLs Using the ACL Editor	24-7
24.3	Using ACLs	24-8
24.3.1	Applying ACLs to Interfaces	24-8
24.3.2	Applying ACLs to Services	24-9
24.3.3	Applying ACLs to Layer-4 Bridging Ports	24-9
24.3.4	Using ACLs as Profiles	24-10
24.4	Enabling ACL Logging	24-14
24.5	Monitoring ACLs	24-15
25	Security Configuration	25-1
25.1	Configuring RS Access Security	25-1
25.1.1	Configuring RADIUS	25-1
25.1.2	Configuring TACACS	25-3
25.1.3	Configuring TACACS+	25-3
25.1.4	Configuring Passwords	25-5
25.1.5	Configuring SSH	25-5
25.2	Layer-2 Security Filters	25-6
25.2.1	Configuring Layer-2 Address Filters	25-7
25.2.2	Configuring Layer-2 Port-to-Address Lock Filters	25-7
25.2.3	Configuring Layer-2 Static Entry Filters	25-8
25.2.4	Configuring Layer-2 Secure Port Filters	25-8

25.2.5	Monitoring Layer-2 Security Filters	25-9
25.2.6	Layer-2 Filter Examples.	25-9
25.3	Layer-3 Access Control Lists (ACLs).	25-12
25.4	Layer-4 Bridging and Filtering	25-12
25.4.1	Creating an IP or IPX VLAN for Layer-4 Bridging	25-13
25.4.2	Placing the Ports on the Same VLAN	25-14
25.4.3	Enabling Layer-4 Bridging on the VLAN	25-14
25.4.4	Creating ACLs to Specify Selection Criteria for Layer-4 Bridging	25-14
25.4.5	Applying a Layer-4 Bridging ACL to a Port	25-15
25.4.6	Notes	25-15
26	QoS Configuration	26-1
26.1	Layer-2, Layer-3 and Layer-4 Flow Specification	26-2
26.2	Precedence for Layer-3 Flows.	26-2
26.3	RS Queuing Policies	26-3
26.4	Traffic Prioritization for Layer-2 Flows	26-3
26.4.1	Configuring Layer-2 QoS	26-4
26.4.2	802.1p Class of Service Priority Mapping.	26-4
26.5	Traffic Prioritization for Layer-3 & Layer-4 Flows	26-6
26.5.1	Configuring IP QoS Policies	26-6
26.5.2	Configuring IPX QoS Policies.	26-7
26.6	Configuring RS Queuing Policy	26-7
26.6.1	Allocating Bandwidth for a Weighted-Fair Queuing Policy	26-8
26.7	Weighted Random Early Detection (WRED)	26-8
26.7.1	WRED's Effect on the Network	26-8
26.7.2	Weighting Algorithms in WRED.	26-9
26.8	ToS Rewrite.	26-10
26.8.1	Configuring ToS Rewrite for IP Packets	26-11
26.9	Monitoring QoS.	26-12
26.10	Limiting Traffic Rate	26-13
26.10.1	Rate Limiting Modes	26-14
26.10.2	Per-Flow Rate Limiting	26-15
26.10.3	Software-Based Flow-Aggregate Rate Limiting	26-15
26.10.4	Port Rate Limiting	26-16
26.10.5	Aggregate Rate Limiting	26-17
26.10.6	Example Configurations	26-18
26.10.7	Displaying Rate Limit Information	26-19
27	Performance Monitoring.	27-1
27.1	Configuring the RS for Port Mirroring	27-2
27.2	Monitoring Broadcast Traffic	27-3
28	RMON Configuration	28-1
28.1	Configuring and Enabling RMON	28-1
28.1.1	Example of RMON Configuration Commands	28-2
28.1.2	RMON Groups.	28-2

28.1.3	Control Tables	28-4
28.2	Using RMON.	28-5
28.3	Configuring RMON Groups	28-6
28.3.1	Configuration Examples.....	28-8
28.4	Displaying RMON Information.....	28-9
28.4.1	RMON CLI Filters	28-10
28.5	Troubleshooting RMON	28-12
28.6	Allocating Memory to RMON.....	28-13
29	LFAP Configuration Guide	29-1
29.1	Overview	29-1
29.2	Requirements.....	29-1
29.3	Traffic Accounting Services	29-1
29.4	Configuring the LFAP Agent on the RS	29-2
29.5	Monitoring the LFAP Agent on the RS.....	29-3
30	WAN Configuration	30-1
30.1	High-Speed Serial Interface (HSSI) and Standard Serial Interfaces.....	30-1
30.2	Configuring WAN Interfaces	30-1
30.2.1	Primary and Secondary Addresses.....	30-2
30.2.2	Static, Mapped, and Dynamic Peer IP/IPX Addresses.....	30-2
30.2.3	Forcing Bridged Encapsulation	30-3
30.2.4	Packet Compression.....	30-4
30.2.5	Packet Encryption.....	30-5
30.2.6	WAN Quality of Service	30-5
30.3	Frame Relay Overview	30-7
30.3.1	Virtual Circuits.....	30-7
30.3.2	Permanent Virtual Circuits (PVCs)	30-7
30.4	Configuring Frame Relay Interfaces for the RS	30-8
30.4.1	Defining the Type and Location of a Frame Relay and VC Interface	30-8
30.4.2	Setting up a Frame Relay Service Profile.....	30-8
30.4.3	Applying a Service Profile to an Active Frame Relay WAN Port.....	30-9
30.5	Monitoring Frame Relay WAN Ports	30-9
30.6	Frame Relay Port Configuration	30-10
30.7	Point-to-Point Protocol (PPP) Overview.....	30-10
30.7.1	Use of LCP Magic Numbers	30-11
30.8	Configuring PPP Interfaces	30-11
30.8.1	Defining the Type and Location of a PPP Interface.....	30-11
30.8.2	Setting up a PPP Service Profile	30-12
30.8.3	Applying a Service Profile to an Active PPP Port	30-12
30.8.4	Configuring Multilink PPP Bundles.....	30-13
30.9	Monitoring PPP WAN Ports	30-13
30.10	PPP Port Configuration	30-14
30.11	Cisco HDLC WAN Port Configuration.....	30-15

30.11.1	Setting up a Cisco HDLC Service Profile	30-15
30.11.2	Applying a Service Profile to an Active Cisco HDLC WAN Port	30-15
30.11.3	Monitoring Cisco HDLC Port Configuration	30-16
30.12	WAN Rate Shaping.	30-16
30.12.1	Using WAN Rate Shaping.	30-16
30.12.2	WAN Rate-Shaping Policies	30-17
30.12.3	Applying WAN Rate Shaping	30-17
30.12.4	WAN Rate Shaping Configuration Examples	30-18
30.13	WAN Configuration Examples	30-20
30.13.1	Simple Configuration File	30-20
30.13.2	Multi-Router WAN Configuration.	30-20
30.14	Channelized T1 and T3 Services Overview	30-25
30.14.1	T1 WAN Line Card	30-25
30.14.2	Channelized T3 Line Card	30-26
30.14.3	Configuring T1 and T3 Interfaces	30-27
30.14.4	Bit Error Rate Testing	30-29
30.15	Channelized T1 and T3 Example Configurations.	30-31
30.15.1	Bridged MSP MTU/MDU Aggregation	30-31
30.15.2	Routed Inter-Office Connections.	30-34
30.15.3	Routed Metropolitan Backbone	30-39
31	Service Configuration.	31-1
31.1	Service Facility Rate Limiting Types	31-2
31.2	Creating a Service	31-3
31.2.1	Aggregate Rate Limiting Service.	31-3
31.2.2	Flow-Aggregate Rate Limiting Service.	31-3
31.2.3	Per-Flow Rate Limiting Service	31-4
31.2.4	Burst-Safe Rate Limiting Service	31-5
31.3	Applying a Service	31-5
31.3.1	Applying Services With ACLs	31-5
31.3.2	Applying Services Using the MF-Classifer Command	31-6
31.4	Showing a Service.	31-7
31.4.1	Aggregate, Flow-Aggregate, Per-Flow, and Burst-Safe Show Commands.	31-7
31.4.2	Show All Command.	31-8
31.5	Service Configuration Examples.	31-9
31.5.1	Applying a Service to Multiple Servers.	31-9

5.12 TUNNELING VLAN PACKETS ACROSS MANs

The “stackable” VLAN feature on the RS allows you to tunnel multiple VLANs through a metropolitan area network (MAN) over a single backbone VLAN. This feature provides the following benefits:

- Traffic for multiple VLANs, or traffic for multiple customers, can be aggregated to run through a MAN over a single backbone VLAN. The RS supports a maximum of 4094 customers or VLANs and up to 4094 backbone VLANs.
- Spanning tree and rapid spanning tree protocols can be run in customer-specific VLANs; no reconfiguration of customer-specific VLANs is needed.
- Per-VLAN spanning tree can be run in the backbone VLAN.

5.12.1 Stackable VLAN Components

The following figure illustrates the basic components of the stackable VLAN. Routers R1 and R2 switch traffic for customers C1 and C2 through the MAN. Ports et.2.1 on R1 and et.6.1 on R2 belong to customer C1’s VLAN, “BLUE” while ports et.3.1 on R1 and et. 7.1 on R2 belong to customer C2’s VLAN, “GREEN.” Traffic entering any of these four ports are tagged with the appropriate customer VLAN ID (BLUE or GREEN) in an IEEE 802.1q header.

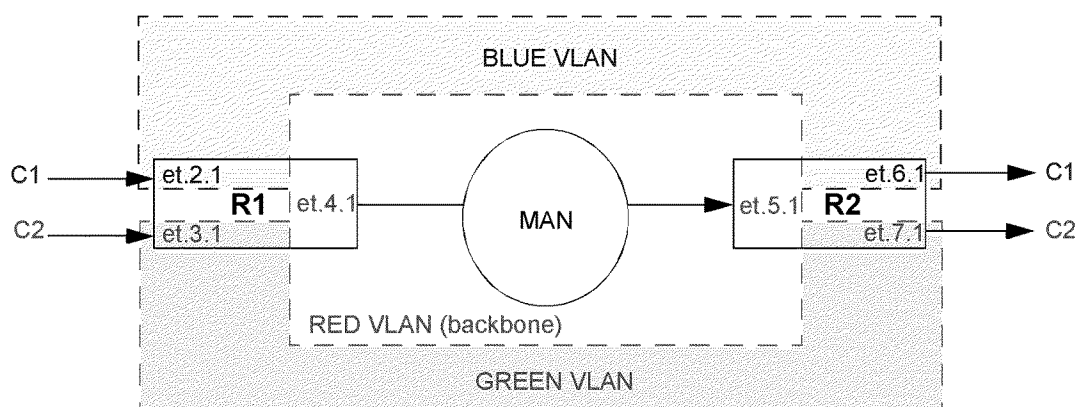


Figure 5-3 Stackable VLAN components

- The VLAN RED is the *backbone VLAN*, which allows traffic from various VLANs to be tunneled through the MAN.
- Ports et.4.1 on R1 and et.5.1 on R2 are *tunnel backbone ports*, which are trunk ports through which the VLAN traffic is tunneled. **Tunnel backbone ports must be configured as trunk ports so that they maintain the encapsulated 802.1q header.** You configure these ports as both trunk ports and tunnel backbone ports with the `stackable-vlan` option of the `vlan make trunk-port` CLI command.
- Ports et.2.1 and et.3.1 on R1 are *tunnel entry ports*, which are access ports on which the VLAN traffic to be tunneled enters R1. Ports et. 6.1 and et.7.1 on R2 are *tunnel exit ports*, which are access ports on which the tunneled traffic exits R2. You configure the mapping of the tunnel entry and tunnel exit ports to the backbone VLAN with the `vlan enable stackable-vlan` CLI command.



Note Tunnel entry and exit port are configured as access ports. These ports can receive 802.1q-tagged traffic.

In Figure 5-3, customer C1 tags outgoing traffic with the VLAN ID BLUE in the 802.1q headers. Customer C1's traffic enters the tunnel entry port et.2.1 on R1. On R1, the tunnel entry port et.2.1 is mapped to the backbone VLAN RED. The BLUE-tagged packet received on port et.2.1 is encapsulated with an 802.1q header with VLAN RED's tag before it is bridged out on the tunnel backbone port et.4.1. (The original 802.1q header with the VLAN BLUE ID is now part of the data portion of the packet.) On R2, the RED 802.1q header is stripped off before the packet is sent out on et.6.1. The packet is sent out the tunnel exit port as a tagged packet with the original BLUE 802.1q header.

If an untagged packet arrives on a tunnel entry port, normal layer 2 processing takes place. If the packet needs to be flooded, it will be flooded on all ports in the customer VLAN.

If a broadcast or multicast packet arrives on a tunnel entry port, the packet is flooded on all ports that belong to the backbone VLAN as well as any other ports that belong to that VLAN. If a unicast packet arrives on a tunnel entry port, the packet is sent out a particular backbone VLAN port.

The 802.1p priority of a packet is preserved throughout the MAN. The RS hardware uses the control priority in the L2 table entry. If there is no L2 table entry for the packet, the 802.1p priority contained in the 802.1q header is used.

Normally, access ports can belong to only one VLAN of a particular protocol type, such as IP. The RS allows tunnel entry and exit ports to be added to multiple VLANs. Note, however, that only ports that are configured with the `stackable-vlan` option of the `vlan make access-port` command can be added to more than one VLAN of the same protocol type.

GARP and/or GVRP can be enabled on tunnel backbone ports.



Note You *cannot* enable L4 bridging on stackable VLANs. Also, do not use the `stp set vlan-disable` command on routers where you are configuring stackable VLANs.

5.12.2 Configuration Examples

This section contains configuration examples for the following scenarios:

- Multiple customers, with each customer having its own VLAN
- Multiple customers sharing a common VLAN
- Single VLAN with multiple tunnel entry ports
- STP or GVRP in customer VLANs tunneled over the backbone VLAN
- Multiple VLANs on a single tunnel entry/exit port

Multiple Customer VLANs

In Figure 5-4, traffic for customer C1's VLAN (BLUE) and for customer C2's VLAN (GREEN) is tunneled through the backbone VLAN (RED).

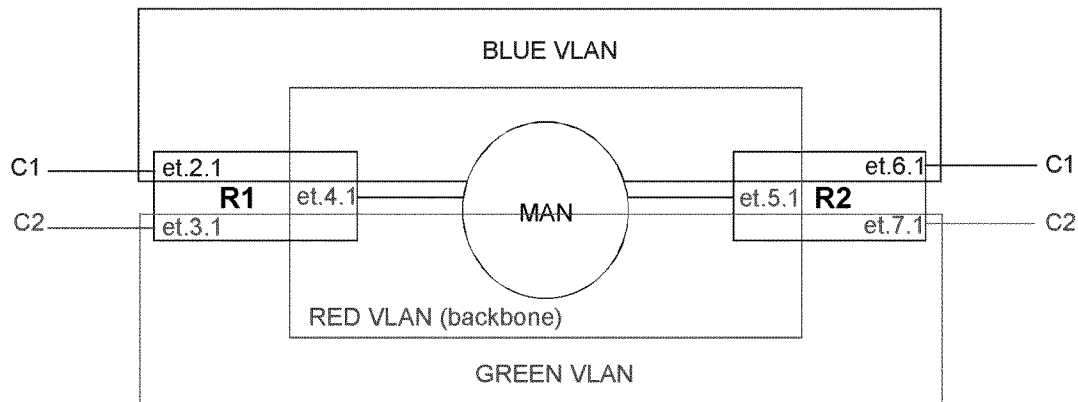


Figure 5-4 Multiple customers with different VLANs

The following is the configuration for R1:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.2.1 to BLUE
vlan add ports et.3.1 to GREEN
vlan add ports et.4.1 to RED
! Make et.4.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.4.1 stackable-vlan
! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan RED
vlan enable stackable-vlan on et.3.1 backbone-vlan RED
```

The following is the configuration for R2:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.6.1 to BLUE
vlan add ports et.7.1 to GREEN
vlan add ports et.5.1 to RED
! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
vlan enable stackable-vlan on et.7.1 backbone-vlan RED
```

Multiple Customers with Common VLANs

In Figure 5-5, customers C1 and C2 are connected to the MAN, with both customers using the same VLAN (BLUE). To ensure that traffic for C1 is not sent to C2 and vice versa, the backbone VLAN for each customer must be different. Therefore, traffic for customer C1 will be sent on the backbone VLAN RED, while traffic for customer C2 will be sent on the backbone VLAN GREEN. Note that the trunk port on each router is part of both backbone VLAN RED and backbone VLAN GREEN.

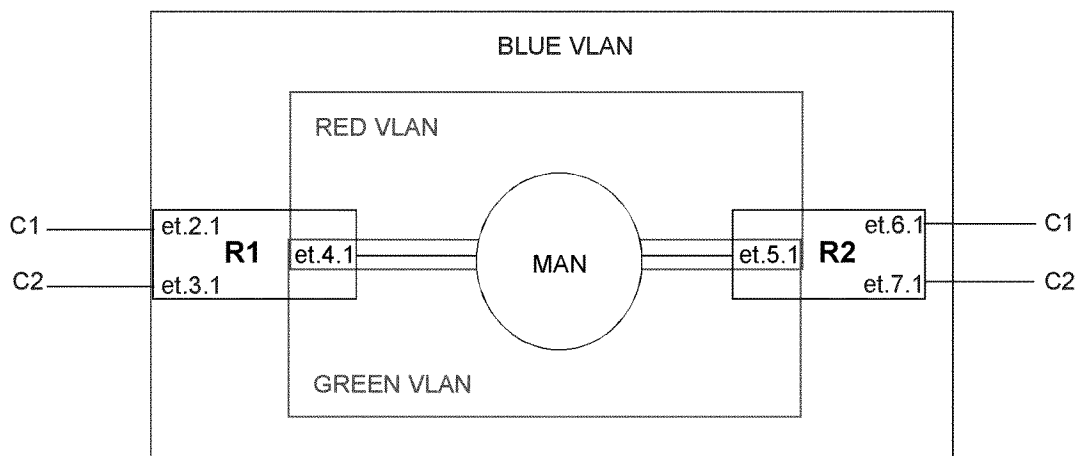


Figure 5-5 Multiple customers with common VLANs

The following is the configuration for R1:

```
! Create 2 backbone VLANs and 1 customer VLAN
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add ports to BLUE VLAN
vlan add ports et.2.1, et.3.1 to BLUE
! Make et.4.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.4.1 stackable-vlan
! Add et.4.1 to both RED and GREEN backbone VLANs
vlan add ports et.4.1 to RED
vlan add ports et.4.1 to GREEN
! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan RED
vlan enable stackable-vlan on et.3.1 backbone-vlan GREEN
```

The following is the configuration for R2:

```
! Create 2 backbone VLANs and 1 customer VLAN
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add ports to BLUE VLAN
vlan add ports et.6.1, et.7.1 to BLUE
! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan
! Add et.5.1 to both RED and GREEN backbone VLANs
vlan add ports et.5.1 to RED
vlan add ports et.5.1 to GREEN
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
vlan enable stackable-vlan on et.7.1 backbone-vlan GREEN
```

Tunnel entry or exit ports can be spread across routers. In Figure 5-6, customers C1 and C3 use the VLAN BLUE, while customers C2 and C4 use the VLAN GREEN. The backbone VLAN for each customer must be different to ensure that traffic for C1 is not sent to C3, traffic for C2 is not sent to C4, etc. Therefore, traffic for customer C1 and C2 will be sent on the backbone VLAN RED, while traffic for customer C3 and C4 will be sent on the backbone VLAN PURPLE.

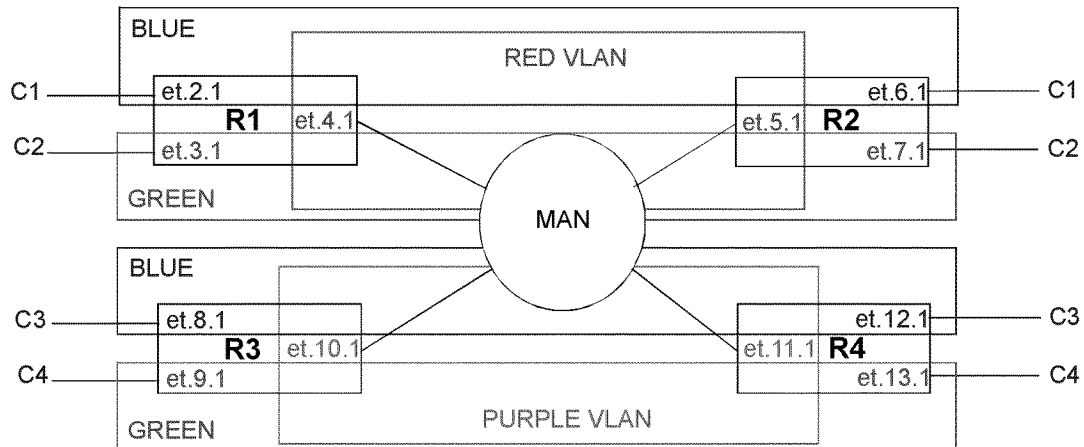


Figure 5-6 Multiple customers with common VLANs across multiple routers

The following is the configuration for R1:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.2.1 to BLUE
vlan add ports et.3.1 to GREEN
vlan add ports et.4.1 to RED
! Make et.4.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.4.1 stackable-vlan
! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan RED
vlan enable stackable-vlan on et.3.1 backbone-vlan RED
```

The following is the configuration for R2:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.6.1 to BLUE
vlan add ports et.5.1 to RED
vlan add ports et.7.1 to GREEN
! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
vlan enable stackable-vlan on et.7.1 backbone-vlan RED
```

The following is the configuration for R3:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create PURPLE port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.8.1 to BLUE
vlan add ports et.9.1 to GREEN
vlan add ports et.10.1 to PURPLE
! Make et.10.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.10.1 stackable-vlan
! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.8.1 backbone-vlan PURPLE
vlan enable stackable-vlan on et.9.1 backbone-vlan PURPLE
```

The following is the configuration for R4:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create PURPLE port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.11.1 to PURPLE
vlan add ports et.12.1 to BLUE
vlan add ports et.13.1 to GREEN
! Make et.11.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.11.1 stackable-vlan
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.12.1 backbone-vlan PURPLE
vlan enable stackable-vlan on et.13.1 backbone-vlan PURPLE
```

Single VLAN with Multiple Tunnel Entry Ports

In Figure 5-7, customer C1 has a VLAN BLUE with multiple tunnel entry ports (et.2.1 and et.3.1 on R1) and multiple tunnel exit ports (et.6.1 and et.7.1 on R2).

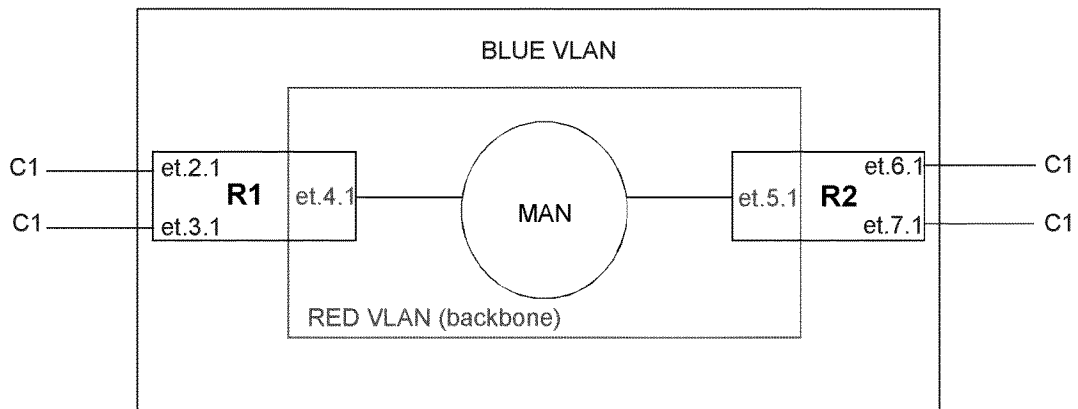


Figure 5-7 Customer VLAN with multiple tunnel entry/exit ports

The following is the configuration for R1:

```
! Create backbone VLAN and customer VLAN
vlan create RED port-based
vlan create BLUE port-based
! Add ports to VLANs
vlan add ports et.2.1, et.3.1 to BLUE
vlan add ports et.4.1 to RED
! Make et.4.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.4.1 stackable-vlan
! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan RED
vlan enable stackable-vlan on et.3.1 backbone-vlan RED
```

The following is the configuration for R2:

```
! Create backbone VLAN and customer VLAN
vlan create RED port-based
vlan create BLUE port-based
! Add ports to VLANs
vlan add ports et.6.1, et.7.1 to BLUE
vlan add ports et.5.1 to RED
! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
vlan enable stackable-vlan on et.7.1 backbone-vlan RED
```

The following is an example where a customer VLAN has multiple tunnel entry or exit ports spread across routers. Figure 5-8 shows customers C1 and C2 sharing the VLAN BLUE. Traffic for customer C1 can arrive on tunnel entry ports on routers R1, R2, or R3. Broadcast or multicast traffic arriving on et.2.1 on R1 is tunneled on backbone VLAN RED and will be seen by C1 users on R2 and R3. C2 users on R4 will not see the C1 traffic since the tunnel backbone port on R4 belongs to the backbone VLAN PURPLE.

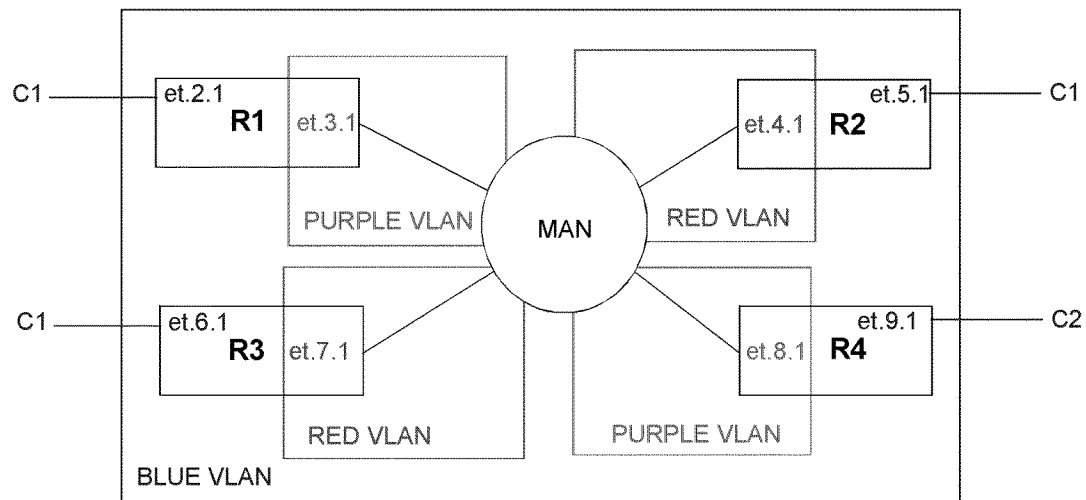


Figure 5-8 Customer VLAN with multiple tunnel entry ports across multiple routers

The following is the configuration for R1:

```
! Create 1 backbone VLAN and 1 customer VLAN
vlan create PURPLE port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.2.1 to BLUE
vlan add ports et.3.1 to PURPLE
! Make et.3.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.3.1 stackable-vlan
! Map tunnel entry port to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan PURPLE
```

The following is the configuration for R2:

```
! Create 1 backbone VLAN and 1 customer VLAN  
vlan create RED port-based  
vlan create BLUE port-based  
! Add port to each VLAN  
vlan add ports et.4.1 to RED  
vlan add ports et.5.1 to BLUE  
! Make et.4.1 both a trunk port and a tunnel backbone port  
vlan make trunk-port et.4.1 stackable-vlan  
! Map tunnel exit ports to backbone VLAN  
vlan enable stackable-vlan on et.5.1 backbone-vlan RED
```

The following is the configuration for R3:

```
! Create 1 backbone VLAN and 1 customer VLAN  
vlan create RED port-based  
vlan create BLUE port-based  
! Add port to each VLAN  
vlan add ports et.6.1 to BLUE  
vlan add ports et.7.1 to RED  
! Make et.7.1 both a trunk port and a tunnel backbone port  
vlan make trunk-port et.7.1 stackable-vlan  
! Map tunnel entry ports to backbone VLAN  
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
```

The following is the configuration for R4:

```
! Create 1 backbone VLAN and 1 customer VLAN  
vlan create PURPLE port-based  
vlan create BLUE port-based  
! Add port to each VLAN  
vlan add ports et.8.1 to PURPLE  
vlan add ports et.9.1 to BLUE  
! Make et.8.1 both a trunk port and a tunnel backbone port  
vlan make trunk-port et.8.1 stackable-vlan  
! Map tunnel exit ports to backbone VLAN  
vlan enable stackable-vlan on et.9.1 backbone-vlan PURPLE
```



Note If you do not want multicast or broadcast traffic from C1 on R1 to be seen by C1 on R3, then configure a different backbone VLAN on R3.

STP/GVRP in Customer VLANs Tunneled over Backbone VLAN

STP, RSTP, or GARP/GVRP can be run in the customer VLANs which are tunneled over the backbone VLAN. The customer VLAN does not need to be reconfigured in order to be tunneled.

In Figure 5-9, traffic for customer C1's VLAN (BLUE) and for customer C2's VLAN (GREEN) is tunneled through the backbone VLAN (RED). STP is enabled in the customer VLAN BLUE on the customer routers C1R1 and C1R2 for customer C1.

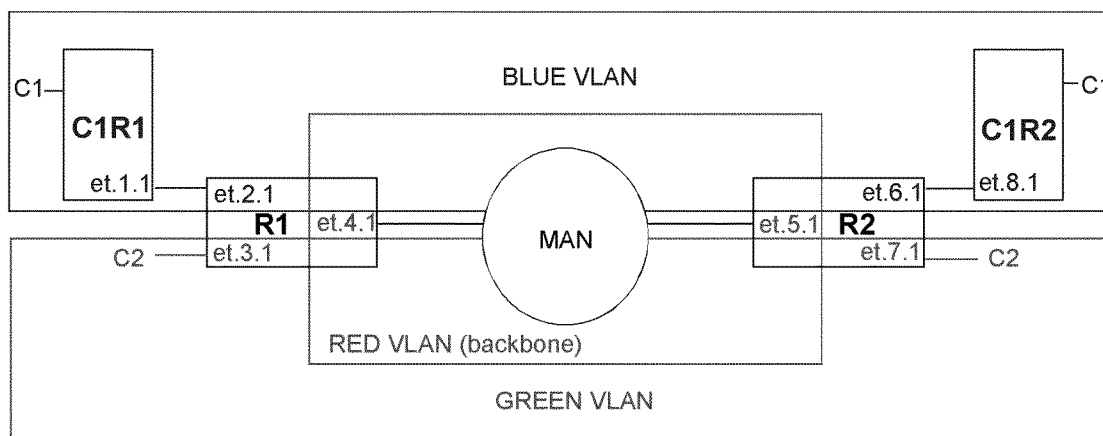


Figure 5-9 STP enabled in customer VLANs

The following configuration statements on C1R1 enable STP on port et.1.1, the port that is connected to the tunnel entry port.

```
! Create customer VLAN
vlan create BLUE port-based

! Add port to VLAN
vlan add ports et.1.1 to BLUE

! Make port et.1.1 a trunk port
vlan make trunk-port et.1.1

! Enable STP on et.1.1
stp enable port et.1.1

! Optional STP configurations
stp set bridging hello-time 3
```

The following configuration statements on C1R2 enable STP on port et.8.1, the port that is connected to the tunnel exit port.

```
! Create customer VLAN  
vlan create BLUE port-based  
! Add port to VLAN  
vlan add ports et.8.1 to BLUE  
! Make port et.8.1 a trunk port  
vlan make trunk-port et.8.1  
! Enable STP on et.8.1  
stp enable port et.8.1
```

The configuration of the tunnel entry/exit ports and tunnel backbone ports on R1 and R2 are identical to those shown in the earlier example in Figure 5-4:

The following is the configuration for R1:

```
! Create 1 backbone VLAN and 2 customer VLANs  
vlan create RED port-based  
vlan create GREEN port-based  
vlan create BLUE port-based  
! Add port to each VLAN  
vlan add ports et.2.1 to BLUE  
vlan add ports et.3.1 to GREEN  
vlan add ports et.4.1 to RED  
! Make et.4.1 both a trunk port and a tunnel backbone port  
vlan make trunk-port et.4.1 stackable-vlan  
! Map tunnel entry ports to backbone VLAN  
vlan enable stackable-vlan on et.2.1 backbone-vlan RED  
vlan enable stackable-vlan on et.3.1 backbone-vlan RED
```

The following is the configuration for R2:

```
! Create 1 backbone VLAN and 2 customer VLANs
vlan create RED port-based
vlan create GREEN port-based
vlan create BLUE port-based
! Add port to each VLAN
vlan add ports et.6.1 to BLUE
vlan add ports et.7.1 to GREEN
vlan add ports et.5.1 to RED
! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan
! Map tunnel exit ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
vlan enable stackable-vlan on et.7.1 backbone-vlan RED
```

Multiple VLANs on a Single Tunnel Entry Port

Tunnel entry and exit ports are access ports. Normally, access ports can belong to only one VLAN of a particular protocol type. With stackable VLANs, traffic for multiple VLANs can enter a tunnel entry port to be tunneled over the backbone VLAN. In this case, the tunnel entry port must belong to all the VLANs that are to be tunneled. Use the `stackable-vlan` option of the `vlan make access-port` command to allow the tunnel entry port to be added to any number of VLANs.

In Figure 5-10, customers C1, C2, C3, C4, and C5 each have a VLAN that will use port et.2.1 on R1 as the tunnel entry port. On R2, port et.6.1 will be the tunnel exit port for traffic for all five VLANs.

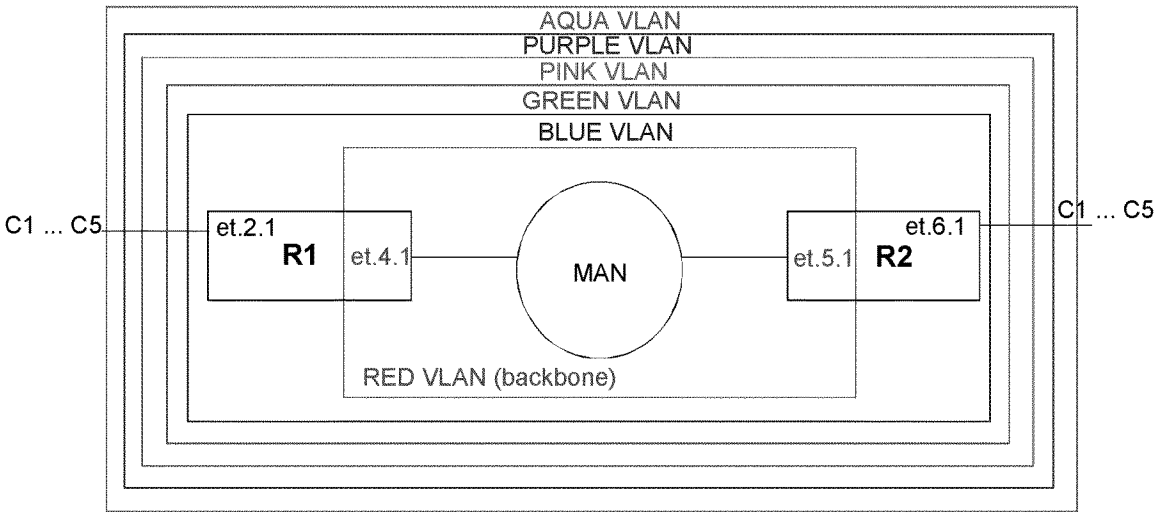


Figure 5-10 Multiple VLANs on single tunnel entry port

The following is the configuration for R1:

```

! Create backbone VLAN
vlan create RED port-based

! Create customer VLANs
vlan create BLUE port-based
vlan create GREEN port-based
vlan create PINK port-based
vlan create PURPLE port-based
vlan create AQUA port-based

! Make et.2.1 an access port that can belong to > 1 VLAN
vlan make access-port et.2.1 stackable-vlan

! Add ports to VLANs
vlan add ports et.2.1 to BLUE
vlan add ports et.2.1 to GREEN
vlan add ports et.2.1 to PINK
vlan add ports et.2.1 to PURPLE
vlan add ports et.2.1 to AQUA

! Add port to backbone VLAN
vlan add ports et.4.1 to RED

! Make et.4.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.4.1 stackable-vlan

! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.2.1 backbone-vlan RED

```



Note

Note that in the above configuration, the commands that add port et.2.1 to more than one VLAN must be issued *before* the command to map the port to the backbone VLAN. That is, the `vlan add ports` commands must occur *before* the `vlan enable stackable-vlan` command. Once the `vlan enable stackable-vlan` command is issued, ports cannot be added to or removed from the customer VLANs.

The following is the configuration for R2:

```
! Create backbone VLAN
vlan create RED port-based

! Create customer VLANs
vlan create BLUE port-based
vlan create GREEN port-based
vlan create PINK port-based
vlan create PURPLE port-based
vlan create AQUA port-based

! Make et.6.1 an access port that can belong to > 1 VLAN
vlan make access-port et.6.1 stackable-vlan

! Add ports to VLANs
vlan add ports et.6.1 to BLUE
vlan add ports et.6.1 to GREEN
vlan add ports et.6.1 to PINK
vlan add ports et.6.1 to PURPLE
vlan add ports et.6.1 to AQUA

! Add port to backbone VLAN
vlan add ports et.5.1 to RED

! Make et.5.1 both a trunk port and a tunnel backbone port
vlan make trunk-port et.5.1 stackable-vlan

! Map tunnel entry ports to backbone VLAN
vlan enable stackable-vlan on et.6.1 backbone-vlan RED
```

5.12.3 Displaying Stackable VLAN Information

Use the `vlan show stackable-vlan` command to display the configuration of stackable VLANs on the RS. For example:

```
rs# vlan show stackable-vlan
Stackable VLAN Information
=====

(20, 222): ❶
  Applied On: et.6.1 ❷
  Flooded On: et.3.8,et.6.1 ❸

Stackable VLAN Trunk Ports: et.3.8 ❹

Stackable VLAN Access Ports: ❺
```

The following explains the display:

1. The ID number of the VLAN, followed by the ID number of the backbone VLAN.
2. The tunnel entry/exit ports, configured with the **vlan enable stackable-vlan** command.
3. The ports on which multicast, broadcast, or unknown unicast packets are flooded.
4. The tunnel backbone ports, configured with the **stackable-vlan** option of the **vlan make trunk-port** command.
5. Tunnel entry ports that have also been configured (with the **stackable-vlan** option of the **vlan make access-port** command) as access ports that can belong to more than one VLAN of the same protocol type. This allows multiple VLANs to use the same tunnel entry port.

